What is an explicit bijection?

Andrej Bauer

Faculty of mathematics and Physics
University of Ljubljana

Institute for mathematics, physics, and mechanics

The 31st International Conference on Formal Power Series and Algebraic Combinatorics
Ljubljana – Slovenia – July 2019

StackExchange Search on MathOverflow…

mathoverflow

What is an explicit bijection in combinatorics?

42

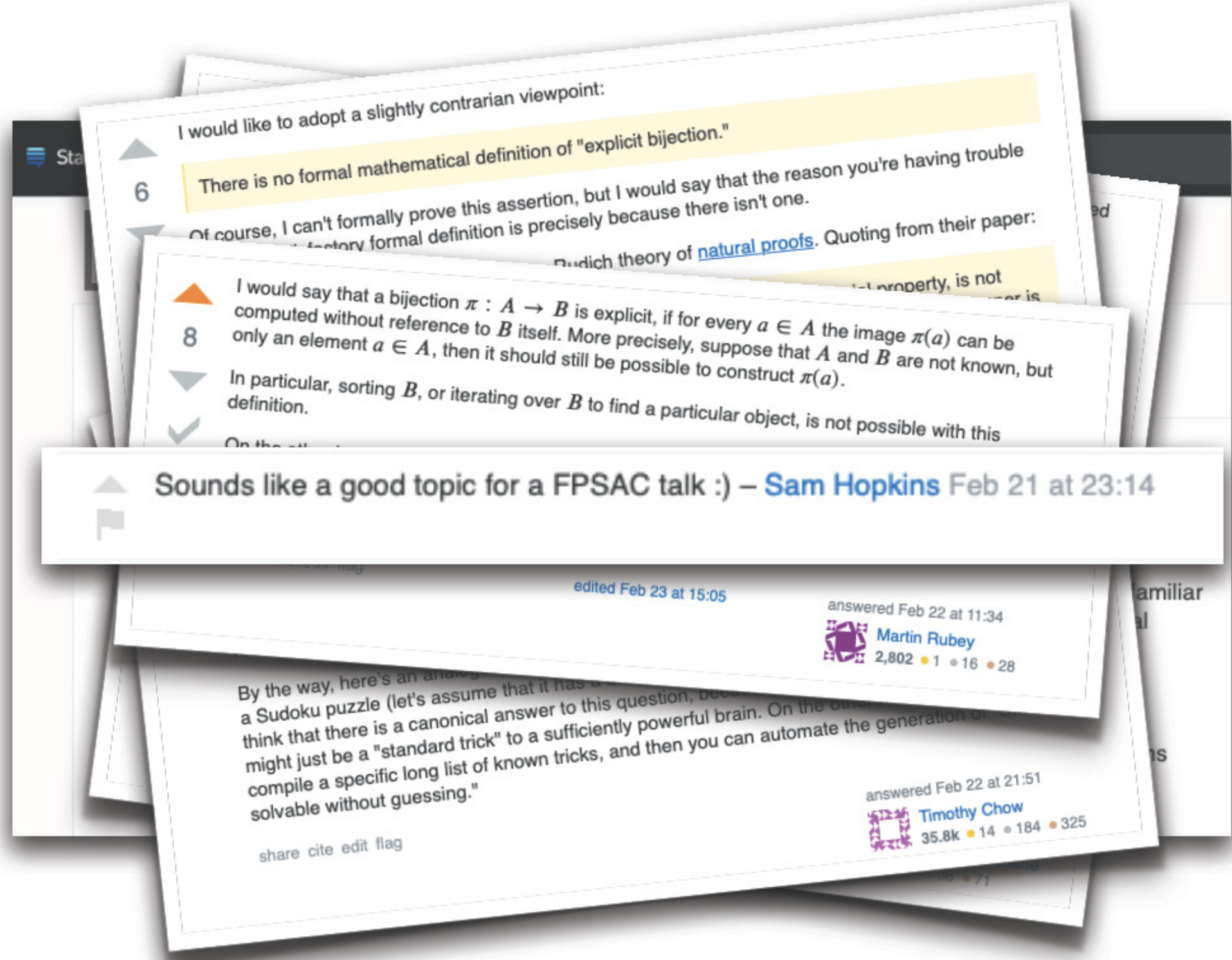
13

A standard way of demonstrating that two collections of combinatorial objects have the same cardinality is to exhibit a bijection between them. Browsing through some examples (here, there, yonder) quickly reveals that combinatorialists call such bijections *explicit*, presumably to differentiate them from other less palpable kinds of bijections. Wikipedia speaks of the method of bijective proof.

It seems that we have here a typical example of an informal mathematical notion that is quite familiar to most mathematicians, however it is difficult to pin down a proper and satisfying mathematical definition. I asked the local combinatorialists and did not really get a good answer.

Question: *What is a proper mathematical definition of an explicit bijection?*

Often we ask for an explicit bijection between two *families* of combinatorial objects, i.e., bijections $b_n : A_n \to B_n$, one for each $n \in \mathbb{N}$. Here $(A_n)_n$ and $(B_n)_n$ are two families of combinatorial objects, parametrized by n. The parameter need not be a single number.


I would like to adopt a slightly contrarian viewpoint:
6
There is no formal mathematical definition of "explicit bijection."
Of course, I can't formally prove this assertion, but I would say that the reason you're having trouble
factory formal definition is precisely because there isn't one.
Rudich theory of natural proofs. Quoting from their paper:
property, is not
I would say that a bijection $\pi : A \to B$ is explicit, if for every $a \in A$ the image $\pi(a)$ can be
8
computed without reference to B itself. More precisely, suppose that A and B are not known, but
only an element $a \in A$, then it should still be possible to construct $\pi(a)$.
In particular, sorting B, or iterating over B to find a particular object, is not possible with this
definition.
On the
Sounds like a good topic for a FPSAC talk :) – Sam Hopkins Feb 21 at 23:14
edited Feb 23 at 15:05
answered Feb 22 at 11:34
Martin Rubey
2,802 • 1 • 16 • 28
familiar
By the way, here's an
a Sudoku puzzle (let's assume that it has
think that there is a canonical answer to this question, bec
might just be a "standard trick" to a sufficiently powerful brain. On the oth
compile a specific long list of known tricks, and then you can automate the generation of
solvable without guessing."
share cite edit flag
answered Feb 22 at 21:51
Timothy Chow
35.8k • 14 • 184 • 325

An explicit bijection $f : A \to B$ is ...

- ... computable in polynomial time.
- ... a natural isomorphism.
- ... computed without reference to B.
- ... given without prior knowledge that $A \cong B$.

An explicit bijection $f : A \to B$ is ...

additional property or structure

- ... computable in polynomial time.
- ... a natural isomorphism.
- ... computed without reference to B.
- ... given without prior knowledge that $A \cong B$.

An explicit bijection $f : A \to B$ is ...

- ... computable in polynomial time.
- ... a natural isomorphism.
- ... computed without reference to B.
- ... given without prior knowledge that $A \cong B$.

the way it is constructed

FOL & ZFC

$$\bot \quad \top \quad \land \quad \lor \quad \Rightarrow \quad \forall \quad \exists$$

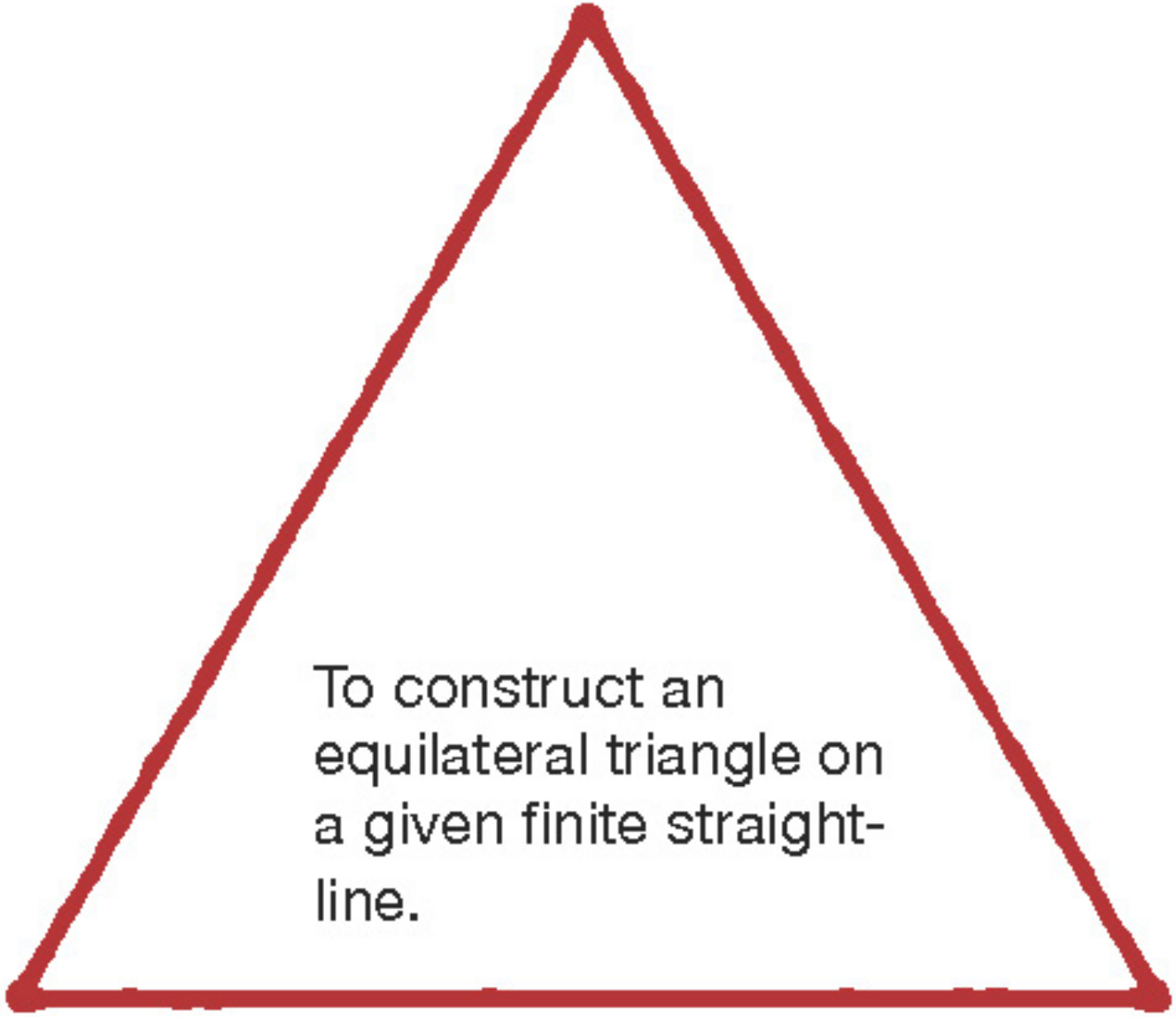
$$\in$$

FOL & ZFC

$$\bot \quad \top \quad \wedge \quad \vee \quad \Rightarrow \quad \forall \quad \exists$$

$$\in \quad \subseteq \quad \varnothing \quad \cap \quad \cup \quad \wp$$

' Επὶ τῆς δοθείσης
εὐθείας πεπερασμένης
τρίγωνον ἰσόπλευρον
συστήσασθαι


To construct an
equilateral triangle on
a given finite straight-
line.

First isomorphism theorem

$$G / \ker \phi \cong \operatorname{im} \phi$$

First isomorphism theorem

$\exists\, \theta : G / \ker \phi \to \operatorname{im} \phi$. θ iso

First isomorphism theorem

$$\exists\, \theta : G / \ker \phi \to \operatorname{im} \phi \;.\; \theta \text{ iso}$$

Proof: Consider the map $\theta : x\,(\ker \phi) \mapsto \phi\, x$.

What would Euclid do?

To construct an isomorphism
$G / \ker \phi \cong \operatorname{im} \phi$

Solution: Consider the map $\theta : x(\ker \phi) \mapsto \phi x$.

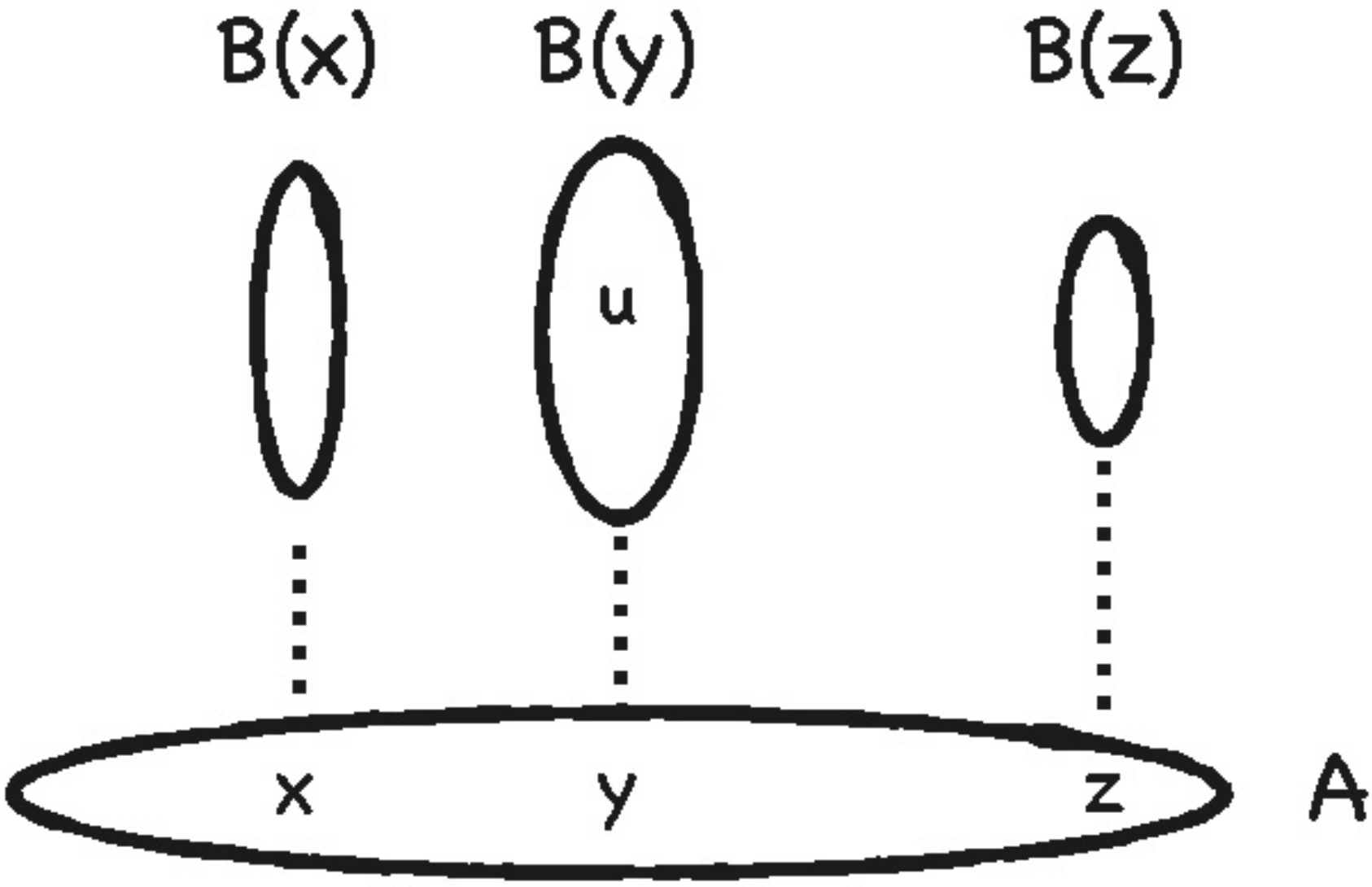
Type theory

$$t : A$$

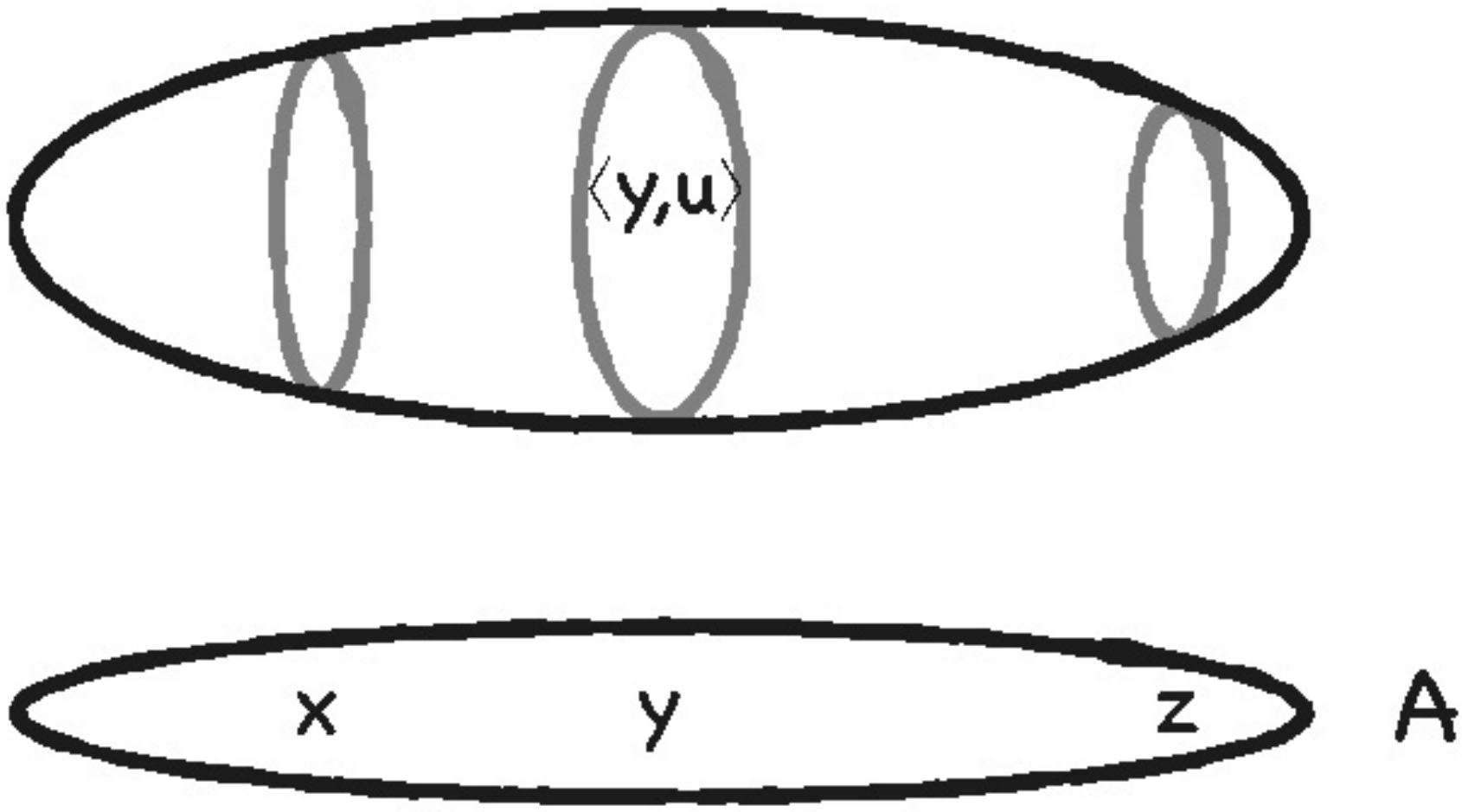
Type theoretic constructions

Type	Element
1	$\langle\rangle$
0	
$\mathbb{N}$	0, succ n
$\mathcal{U}$	A, B
$A \times B$	$\langle a, b \rangle$
$A + B$	$\iota_1(a)$, $\iota_2(b)$
$A \to B$	$x \mapsto e(x)$
$\prod (x : A) . B(x)$	$x \mapsto e(x)$
$\sum (x : A) . B(x)$	$\langle a, b \rangle$

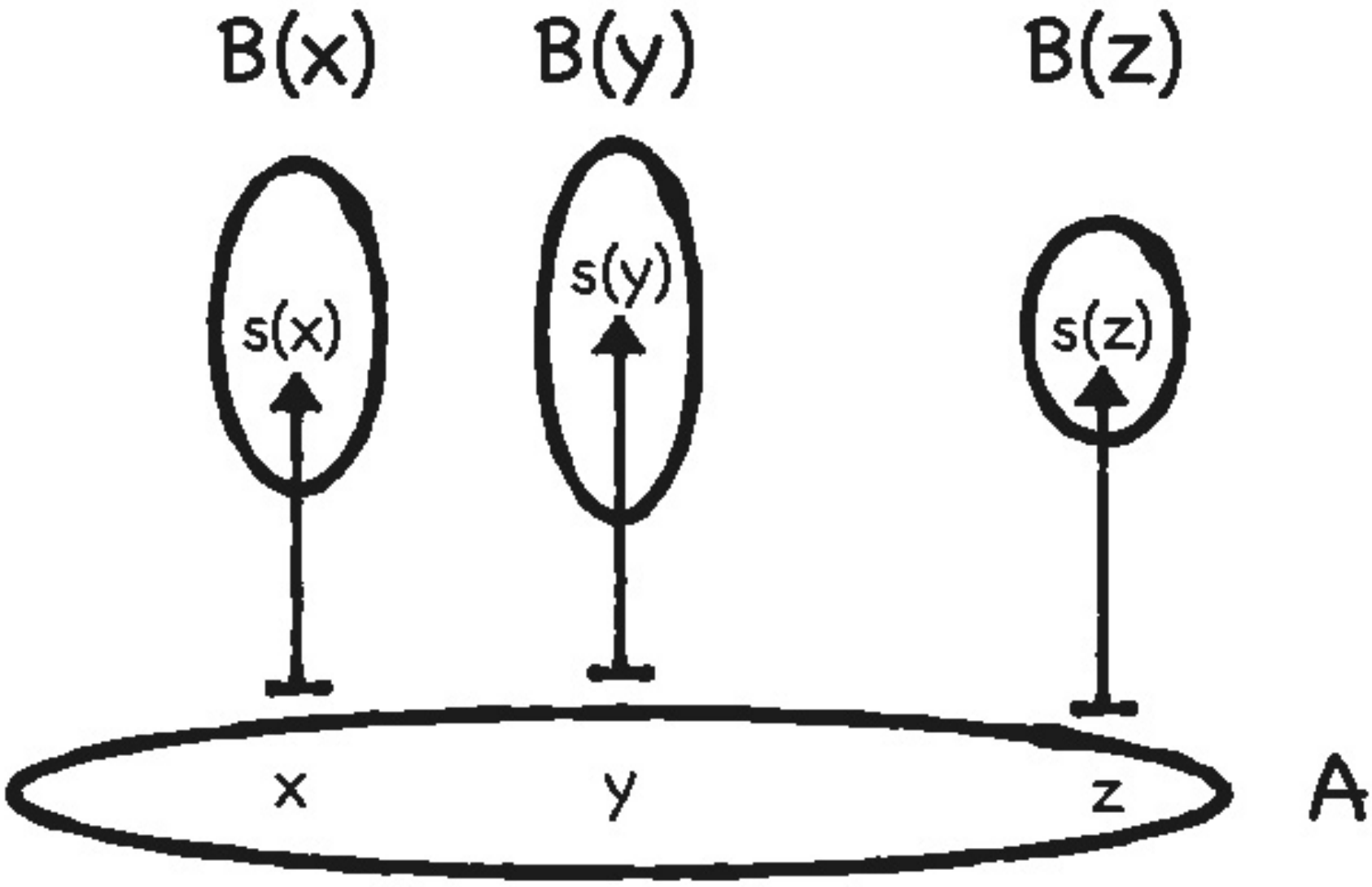
Dependent type B over A



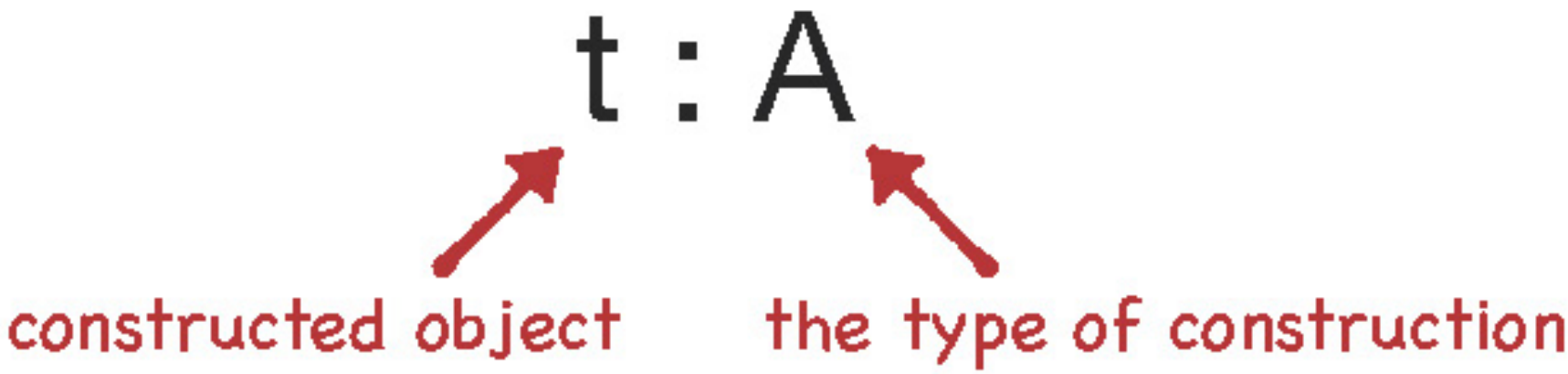
$$\Sigma(x : A).B(x)$$



Π(x : A).B(x)



Where is logic?



Where is logic?

The Curry-Howard correspondence

Logic	Types	Element/proof
$\top$	1	$\langle\rangle$
$\bot$	0	
$A \wedge B$	$A \times B$	$\langle a, b \rangle$
$A \vee B$	$A + B$	$\iota_1(a), \iota_2(b)$
$A \Rightarrow B$	$A \to B$	$x \mapsto e(x)$
$\forall\, x \in A\,.\, B(x)$	$\prod (x : A)\,.\, B(x)$	$x \mapsto e(x)$
$\exists\, x \in A\,.\, B(x)$	$\sum (x : A)\,.\, B(x)$	$\langle a, b \rangle$

The Curry-Howard correspondence

Logic	Types	Element/proof
$\top$	1	$\langle\rangle$
$\bot$	0	
$A \wedge B$	$A \times B$	$\langle a, b \rangle$
$A \vee B$	$A + B$	$\iota_1(a), \iota_2(b)$
$A \Rightarrow B$	$A \to B$	$x \mapsto e(x)$
$\forall\, x \in A\,.\, B(x)$	$\prod (x : A)\,.\, B(x)$	$x \mapsto e(x)$
$\exists\, x \in A\,.\, B(x)$	$\sum (x : A)\,.\, B(x)$	$\langle a, b \rangle$

$$p : \exists\, x \in A \,.\, B(x)$$

cannot extract an element of A from p

$$p : \Sigma\, (x : A) \,.\, B(x)$$

may project an element of A from p

Propositional truncation

Type	Element
$\lVert A \rVert$	$\lvert a \rvert$

"A quotiented by A × A"

"the (only) equivalence class"

The Curry-Howard correspondence

Logic	Types	Element/proof
$\top$	1	$\langle\rangle$
$\bot$	0	
$A \wedge B$	$A \times B$	$\langle a, b \rangle$
$A \vee B$	$A + B$	$\iota_1(a), \iota_2(b)$
$A \Rightarrow B$	$A \to B$	$x \mapsto e(x)$
$\forall\, x \in A\,.\, B(x)$	$\prod (x : A)\,.\, B(x)$	$x \mapsto e(x)$
$\exists\, x \in A\,.\, B(x)$	$\sum (x : A)\,.\, B(x)$	$\langle a, b \rangle$

The Curry-Howard correspondence

Logic	Types	Element/proof
$\top$	1	$\langle\rangle$
$\bot$	0	
$A \wedge B$	$A \times B$	$\langle a, b\rangle$
$A \vee B$	$\|A + B\|$	$\|\iota_1(a)\|, \|\iota_2(b)\|$
$A \Rightarrow B$	$A \to B$	$x \mapsto e(x)$
$\forall\, x \in A\,.\, B(x)$	$\prod (x : A)\,.\, B(x)$	$x \mapsto e(x)$
$\exists\, x \in A\,.\, B(x)$	$\|\sum (x : A)\,.\, B(x)\|$	$\|\langle a, b\rangle\|$

Equality type

Type	Element
$t =_A u$	“path from t to u”

Equality type

Type	Element
$t =_A u$	"path from t to u"
$A =_U B$	"A is equivalent to B"

Univalence axiom:

$(A =_U B) \simeq (A \simeq B)$

"equality is equivalent to equivalence"

$$\Pi\ (n : N)\ .\ \Sigma\ (p : N)\ .\ (n < p) \times \text{prime}(p)$$

Map that takes a number n to $\langle p, \langle q, r \rangle \rangle$ such that p is a number, q proves $n < p$, and r proves prime(p).

For every number to construct a prime larger than it.

$$\Pi\ (n : N)\ .\ \Sigma\ (p : N)\ .\ (n < p) \times \text{prime}(p)$$

Map that takes a number n to $\langle p, \langle q, r \rangle\rangle$ such that p is a number, q proves $n < p$, and r proves prime(p).

For every number to construct a prime larger than it.

$$\Pi\ (n : N)\ .\ \|\Sigma\ (p : N)\ .\ (n < p) \times \text{prime}(p)\|$$

Map that takes a number n to an (abstracted) proof showing that there is a prime larger than n.

For every number there exists a prime larger than it.

Explicit bijection

$$\Sigma\,(f : A \to B)\ \Sigma\,(g : B \to A)\ .\ (f \circ g = id_B) \times (g \circ f = id_A)$$

A quadruple $\langle f, \langle g, \langle p, q \rangle \rangle \rangle$ such that p is a path from $f \circ g$ to id_B and q a path from $g \circ f$ to id_A.

To construct a bijection from A to B.

Non-explicit bijection

$$\|\Sigma\,(f : A \to B)\,\Sigma\,(g : B \to A)\,.\,(f \circ g = \mathrm{id}_B) \times (g \circ f = \mathrm{id}_A)\|$$

A proof $|\langle f, \langle g, \langle p, q\rangle\rangle\rangle|$ such that p is a path from $f \circ g$ to id_B and q a path from $g \circ f$ to id_A.

There exists a bijection from A to B.

$$[n] := \Sigma\ (k : N)\ .\ k < n$$

The numbers 0,1, ..., n-1.

$$[n] := \Sigma\ (k : N)\ .\ k < n$$

The numbers 0,1, ..., n-1.

$$\Sigma\ (A : U)\ \Sigma\ (n : N)\ .\ A \cong [n]$$

Type A with a number n and isomorphism $A \cong [n]$.

$$[n] := \Sigma\ (k : N)\ .\ k < n$$

The numbers 0,1, ..., n-1.

$$\Sigma\ (A : U)\ \Sigma\ (n : N)\ .\ A \cong [n]$$

Type A with a number n and isomorphism $A \cong [n]$.

$$\mathrm{Fin} := \Sigma\ (A : U)\ \|\Sigma\ (n : N)\ .\ A \cong [n]\|$$

Type A such that there exists $A \cong [n]$.

$$[n] := \Sigma\ (k : N)\ .\ k < n$$

The numbers 0,1, ..., n-1.

$$\Sigma\ (A : U)\ \Sigma\ (n : N)\ .\ A \cong [n]$$

Type A with a number n and isomorphism $A \cong [n]$.

$$\mathrm{Fin} := \Sigma\ (A : U)\ \|\Sigma\ (n : N)\ .\ A \cong [n]\|$$

Type A such that there exists $A \cong [n]$.

$$\mathrm{Fin} \to U$$

Combinatorial spices.

$$[n] \to A$$

Ordered n-tuple of elements in A

$$[n] \to A$$

Ordered n-tuple of elements in A

$$\mathrm{Fin}_n := \Sigma\ (A : U)\ \| A \cong \mathrm{Fin}(n) \|$$

Type with n elements.

$$\Sigma\ (B : \mathrm{Fin}_n)\ .\ B \to A$$

Unordered n-tuples of elements in A

$$[n] \to A$$

Ordered n-tuple of elements in A

$$\mathrm{Fin}_n := \Sigma\,(A : U)\ \|A \cong \mathrm{Fin}(n)\|$$

Type with n elements.

$$\Sigma\,(B : \mathrm{Fin}_n)\ .\ B \to A$$

Unordered n-tuples of elements in A

$$\mathrm{Fin}_2$$

The infinite-dimensional real-projective space $\mathbb{RP}^\infty$